(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 October 2003 (23.10.2003)

PCT

(10) International Publication Number
WO 03/088532 A1

(51) International Patent Classification[7]: H04B 17/00

(21) International Application Number: PCT/US03/11107

(22) International Filing Date: 11 April 2003 (11.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/371,938 11 April 2002 (11.04.2002) US

(71) Applicant *(for all designated States except US)*: **THE JOHNS HOPKINS UNIVERSITY** [US/US]; 34th and Charles Streets, Baltimore, MD 21218 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MUADDI, Albert, B.** [US/US]; 11215 Oak Leaf Drive, Apt. 2013, Silver Spring, MD 20901 (US). **TOMKO, Albert, A.** [US/US]; 2385 Steltz Road, New Freedom, PA 17349 (US).

(74) Agents: **ROCA, Benjamin, Y.** et al.; The Johns Hopkins University, Applied Physics Laboratory, 11100 Johns Hopkins Road, Laurel, MD 20723-6099 (US).

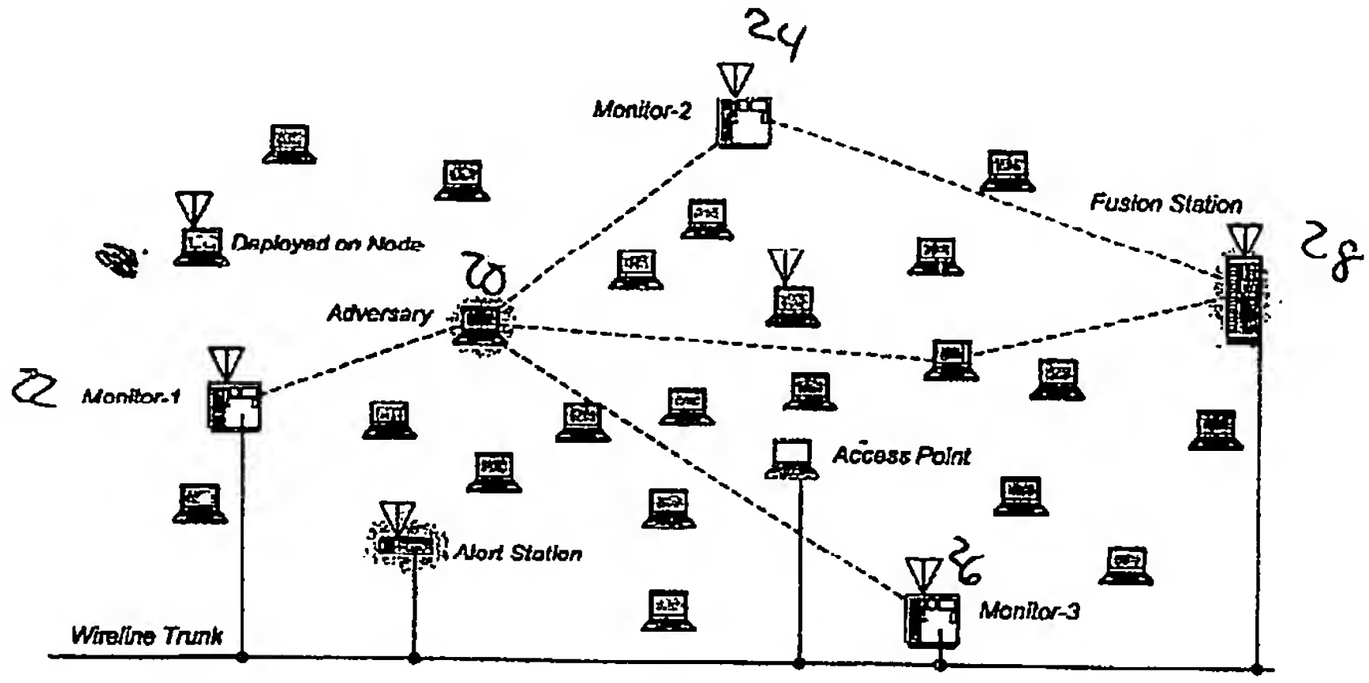
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: INTRUSION DETECTION SYSTEM FOR WIRELESS NETWORKS



(57) Abstract: A method and system (fig. 2) for facilitating detection of intruders into a wireless network, through the use of physical layer anomalies. One or more monitoring stations (22, 24, 26) can be distributed across the potential intruder's signal transmission region. They process these transmissions and extract attributes of the signals, which can then transmit to one or more fusion stations (28), which correlate the calculated attributes with stored attributes of signals of known, authorized users of the network, and transmit alert messages in the case that these signal attributes do not match those of known, authorized users. Signal attributes in accordance with the instant invention include the carrier frequency, spurious emissions, and power-on and power-down transients. Also in accordance with the instant invention are methods and systems using both direct and multipath received signal strength, signal-to-noise ratio, and geometric characteristics such as direction/angle of arrival (AOA), time of arrival, position/range, time dispersion, Doppler shift and polarization.

WO 03/088532 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE OF THE INVENTION

INTRUSION DETECTION SYSTEM FOR WIRELESS NETWORKS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to a provisional application entitled "Wireless Network Physical-layer Intrusion Detection System" filed in the United States Patent and Trademark Office on April 11, 2002 and assigned Serial No. 60/371,938, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention:

[0002] The present invention relates to an intrusion detection system for wireless networks. More specifically, it relates to a method for facilitating detection of intruders into a wireless network, through the use of physical layer anomalies.

Description of the Related Art:

[0003] The use of wireless networks in general, and wireless local area networks (WLANs) in particular, is expanding rapidly, and is now a viable technology for retail stores, hotels, airports, museums, convention centers and college campuses. Being wireless, these networks do not benefit from the same degree of physical security enjoyed by wired networks. However, these networks require robust security measures, for example, accurate monitoring for both unintentional problems and intentional attacks, and intrusion detection systems are an important part of the network architecture.

[0004] Existing intrusion detection systems rely chiefly on network layer and high layer protocol information as inputs to the system. Use of an IPSec client, MAC address authentication, and link layer integrity checks are some conventional techniques in use. While these approaches have utility, they also have limitations. In particular, higher level

techniques such as these are often not robust against certain classes of attacks, for example, datagram spoofing. Spoofing is a class of techniques involving the creation of TCP/IP packets using someone else's IP address. More specific examples include techniques such as man-in-the-middle, routing redirect, source routing, blind spoofing and flooding.

[0005] Thus, what is needed is a method and system in a wireless network for facilitating detection of intruders, which uses physical layer information, thus addressing and solving problems associated with conventional systems using only higher level information.

SUMMARY OF THE INVENTION

[0006] It is one object of the invention disclosed herein to provide a method and system for facilitating detection of intruders into a wireless network, which exploits physical-layer information. By physical layer is meant that layer of the network's protocol architecture concerned with the characteristics of the transmission medium, the nature of the signals, the data rate and related matters.

[0007] The present invention is useful in a variety of applications, where datagram and related spoofing techniques are a concern. One technique employs one or more monitoring stations which may be distributed across the potential intruder's transmission region. These monitoring stations each receive signal transmissions from a local region of the wireless network. They process these transmissions and extract attributes of the signals. They then transmit the processed information (signal attributes) to one or more fusion stations. The fusion stations may correlate the calculated attributes with stored attributes of signals of known, authorized users of the network, and transmit alert messages in the case that these signal attributes do not match those of authorized users of the network.

[0008] Signal attributes in accordance with the instant invention may include intrinsic signal characteristics, such as the carrier frequency, spurious emissions, and power-on and power-down transients. Also in accordance with the instant invention are methods

BNSDOCID: <WO 03088532A1 I >

and systems using both direct and multipath received signal strength (power), signal-to-noise ratio, and geometric characteristics such as direction/angle of arrival (AOA), time of arrival, position/range, time dispersion, Doppler shift and polarization.

[0009] Such signal attributes are generally random variables with time-varying statistics. In general, these statistics will change with orientation, position and velocity of transmitter and receiver, motion of objects within propagation channel, and environmental conditions (e.g. precipitation, smoke, etc.) Therefore, specific implementations of this technique will typically require knowledge of the locations and signal characteristics of known, authorized users, and tuning of the algorithms to these specific details of the situation.

[0010] An advantage of this technique is the ability to "fingerprint" the signal produced by wireless chips. By analyzing and storing specific attributes of signals produced by specific chips, a new level of robustness against intrusion is provided. Intruders who are using different chips than those of known, authorized users may be detected, even though they may be able to pass undetected through higher layers of the network architecture security structure.

[0011] Another advantage of this technique is the capability to identify an intruder by his geographic location. Geometric information may be used to identify an intruder's angle of arrival, range, or other information from which his location may be determined. Signals originating from a location different than that of known, authorized users may be evidence of an intruder.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] **FIG. 1** is a graphical depiction of the layers of a network architecture, and their relationships to an intrusion detection system utilizing physical layer information;

[0013] **FIG. 2** is a graphical representation of an intrusion detection system in accordance with the present invention;

[0014] **FIG 3** displays four graphs of power-on transient signals captured from four PC cards; and

[0015] **FIG 4** shows an original/reconstructed signal of a Cisco PC card, and its wavelet transform.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0016] **FIG. 1** is a graphical depiction of the layers of a network architecture, and their relationships to an intrusion detection system utilizing physical layer information. The specific example here is of a TCP/IP over radio interface.

[0017] Five potential architecture layers are shown in **FIG. 1**. From top to bottom they can be categorized as the application, transport, network, datalink and physical layers. The focus of the present invention is on the physical layer, and the graphics depicts the analog RF signal entering the physical layer, prior to A/D conversion. The most complete intrusion detection system would gather evidence by utilizing all five of the architecture layers. Information from the various layers is fed into models and a decision is made as to the status of an intrusion.

[0018] The present invention is useful in a variety of applications, where datagram and spoofing techniques are a concern. The technique may employ one or more monitoring stations which are distributed across the potential intruder's signal transmission region. These monitoring stations each receive signal transmissions from a local region of the wireless network. They process these transmissions and extract attributes of the signals. They then transmit the processed information (signal attributes) to one or more fusion stations. The fusion stations correlate the calculated attributes with stored attributes of

signals of known, or authorized users of the network, and transmit alert messages in the case that these signal attributes do not match those of authorized users of the network.

[0019] **FIG. 2** is a graphical representation of an intrusion detection system in accordance with the instant invention. Of particular interest to the instant invention are the adversary **20**, three monitoring stations **22, 24, 26**, and a fusion station **28**. The adversary's transmissions may be picked up by one or more monitoring stations, where the RF attributes are estimated and passed to a fusion station. The fusion station correlates this information to detect intrusions. If intrusion is detected, alert packets are sent. Note that this figure is for illustrative purposes only and the number of monitoring stations and fusion stations will vary with the specific network architecture.

[0020] In one class of embodiments of the invention, the monitoring stations receive signals corresponding to power-on or power-down transients of the network participants. Attributes computed by the monitoring stations include characteristics of either Fourier or wavelet-based transforms of the power-on or power-down signals. The monitoring stations may transmit these calculated attributes to one or more fusion stations. The fusion stations then compare the Fourier or wavelet characteristics of the received signals with known Fourier or wavelet characteristics of authorized participants on the network. Anomalies, if detected, cause alert messages to be sent, to notify the appropriate persons or systems that an intruder may be present.

[0021] **FIG 3.** Shows four graphs of power-on transient signals captured from four PC cards, two Lucent cards **30, 32** and two Cisco cards **34, 36**. The graphs shown were obtained through digitization (at 25 MHz IF) of 50 samples of beacon transmission from each of the four cards.

[0022] **FIG 4.** Shows an original/reconstructed signal of a Cisco PC card **40**, and its wavelet transform **42**. Of particular note is the feature of the Cisco card obtained through

the wavelet transform. This is an example of "fingerprinting" of the cards, which can be used to determine a card which is not from a known, authorized user.

[0023] An another embodiment, monitoring stations include a mixer and low power amplifier (LPF) that may obtain an intermediate frequency (IF) signal. Attributes computed by the monitoring stations include statistics on the IF signals in the time domain. These statistics include median, mean and standard deviation. The computed statistics are then transmitted to the fusion station, which compares them to similar stored statistics on signals from known users. Again, anomalies are detected and appropriate authorities are notified.

[0024] In another embodiment, attributes computed by the monitoring stations may include direct path received power, and the ratio of (multipath) power received in-chip to direct path received power. These attributes are then transmitted to the fusion station, which compares them to stored statistics on signals from known users. These stored statistics may include the mean, median and standard deviation of the direct path received power and the ratio of (multipath) power received in-chip to direct path received power. Again, anomalies are detected and appropriate authorities are notified.

[0025] In another embodiment, attributes computed by the monitoring stations include horizontal polarization and/or vertical polarization, and may also include direction of arrival and/or received power. These attributes are then transmitted to the fusion station, which compares them to stored statistics on signals from known users. These stored statistics may include the mean, median and standard deviation of the horizontal polarization and/or vertical polarization, the direction of arrival and/or received power. Again, anomalies are detected and appropriate authorities may be notified.

[0026] Although a specific form of embodiment of the instant invention has been described above and illustrated in the accompanying drawings in order to be more clearly understood, the above description is made by way of example and not as a limitation to the scope of the instant invention. It is contemplated that various modifications apparent to one

of ordinary skill in the art could be made without departing from the scope of the invention which is to be determined by the following claims.

What is claimed is:

1. A system for detecting intrusion into a wireless network, the system comprising:

a monitoring station, having a first transceiver, the first transceiver comprising:

a first receiver front end for receiving and demodulating a first signal,

a first transmitter for sending a first communication, and

a first processor coupled to said first receiver front end for processing the first signal, and coupled to said first transmitter for controlling the first transmitter; and

a fusion station, having a second transceiver, the second transceiver comprising:

a second receiver front end for receiving and demodulating said first communication;

a second transmitter for sending a second communication, and

a second processor coupled to said second receiver front end for processing the first communication from said monitoring station, and said second processor coupled to the second transmitter for controlling the second transmitter.

2. The system of claim 1, wherein

the second processor stores attributes of an expected signal;

the first receiver front end receives and demodulates the first signal;

the first processor calculates attributes of the first signal;

the first transmitter transmits the first communication containing the attributes of the first signal;

the second receiver front end receives and demodulates the first communication;

the second processor compares the attributes of the first signal with the stored attributes of the expected signal to determine whether the attributes of the first signal deviate from the stored attributes of the expected signal; and

the second transmitter transmits alert messages if the attributes of the first signal deviate from the stored attributes of the expected signal.

3. The system of claim 2, wherein the second processor compares a frequency content of power-on transient of the first signal, with a frequency content of power-on transient of the expected signal.

4. The system of claim 2, wherein the second processor compares a stored wavelet transform of power-on transient of the first signal, with a wavelet transform of power-on transient of the expected signal.

5. The system of claim 2, wherein the second processor compares a frequency content of power-down transient of the first signal, with a frequency content of power-down transient of the expected signal.

6. The system of claim 2, wherein the second processor compares a stored wavelet transform of power-down transient of the first signal, with a wavelet transform of power-down transient of the expected signal.

7. The system of claim 2, wherein the second processor compares a median, mean, and standard deviation of an IF signal obtained from the first signal, with a median, mean and standard deviation of an IF signal obtained from the expected signal.

8. The system of claim 2, wherein the second processor compares a direct path received power from the first signal and a ratio of (multipath) power received in-chip to the direct path received power from the first signal, with a direct path received power from the expected signal and the ratio of (multipath) power received in-chip to the direct path received power from the expected signal.

9. The system of claim 2, wherein the second processor compares polarization and direction of arrival of the first signal to polarization and direction of arrival of the expected signal.

10. A method for intrusion detection into a wireless network comprising the steps of:

monitoring a first signal having attributes;

receiving and demodulating a first signal having attributes;

transmitting a first communication;

receiving and demodulating the first communication; and

sending a second communication.

11. The method of claim 10, further comprising the steps of:

storing an expected attribute of an expected signal;

calculating an attribute of the first signal;

comparing an attribute of the first signal with a stored attribute of the expected signal to determine whether the attribute of the first signal deviate from the stored attribute of the expected signal; and

transmitting alert message if the attribute of the first signal deviate from the stored attribute of the expected signal.

12. The method of claim 11, wherein the attribute is a frequency content of power-on transient of the signal.

13. The method of claim 11, wherein the attribute is a wavelet transform of power-on transient of the signal.

14. The method of claim 11, wherein the attribute is a frequency content of power-down transient of the signal.

15. The method of claim 11, wherein the attribute is a wavelet transform of power-down transient of the signal.

16. The method of claim 11, wherein the attribute is a calculated median, mean, or standard deviation of an IF signal obtained from the first signal.

17. The method of claim 11, wherein the attribute is a calculated direct path received power from the signal and a ratio of (multipath) power received in-chip to the direct path received power from the signal.

18. The method of claim 11, wherein the attribute is a calculated polarization and direction of arrival of the signal.

19. The method of claim 11, wherein an attribute includes one or more attributes.

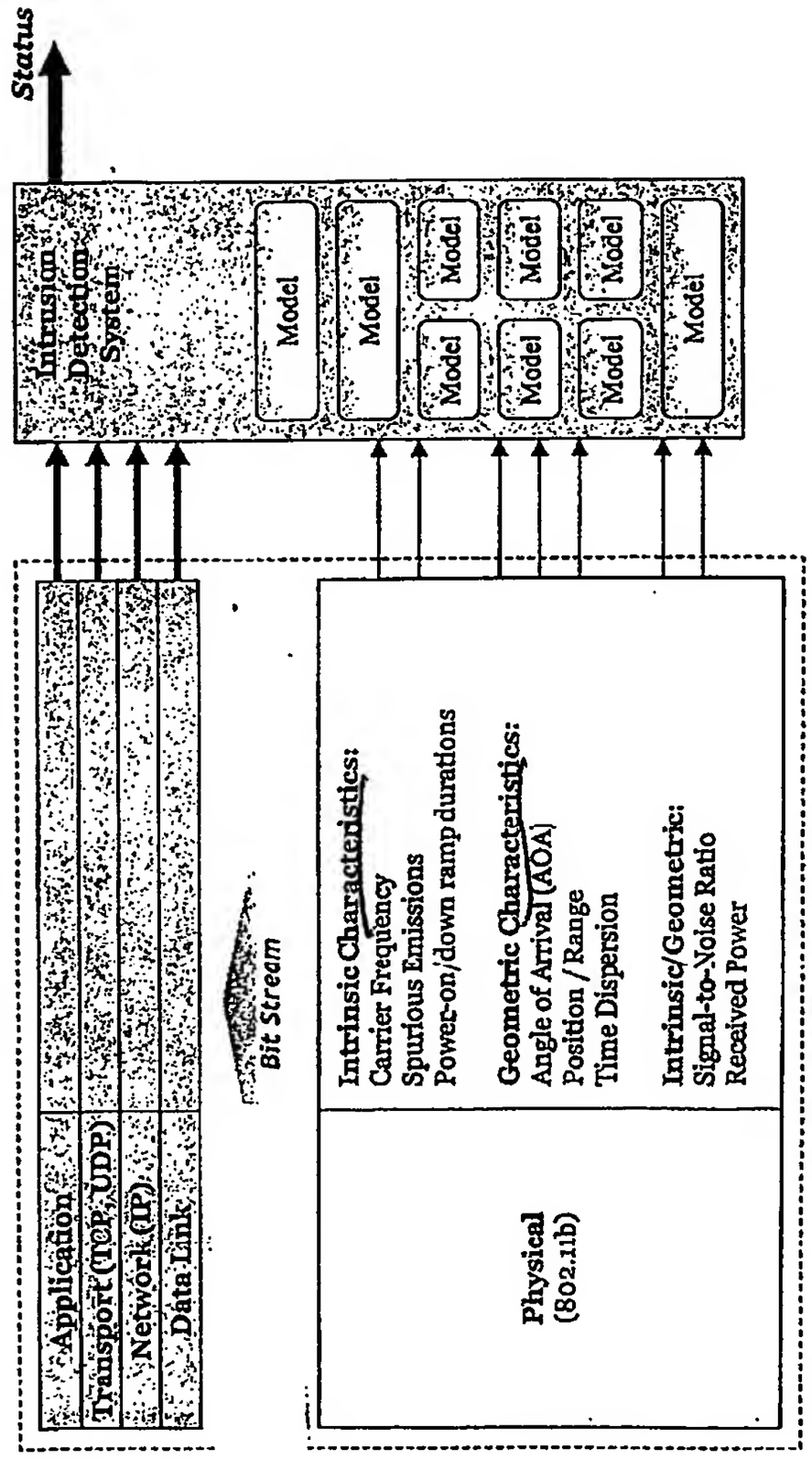


FIGURE 1

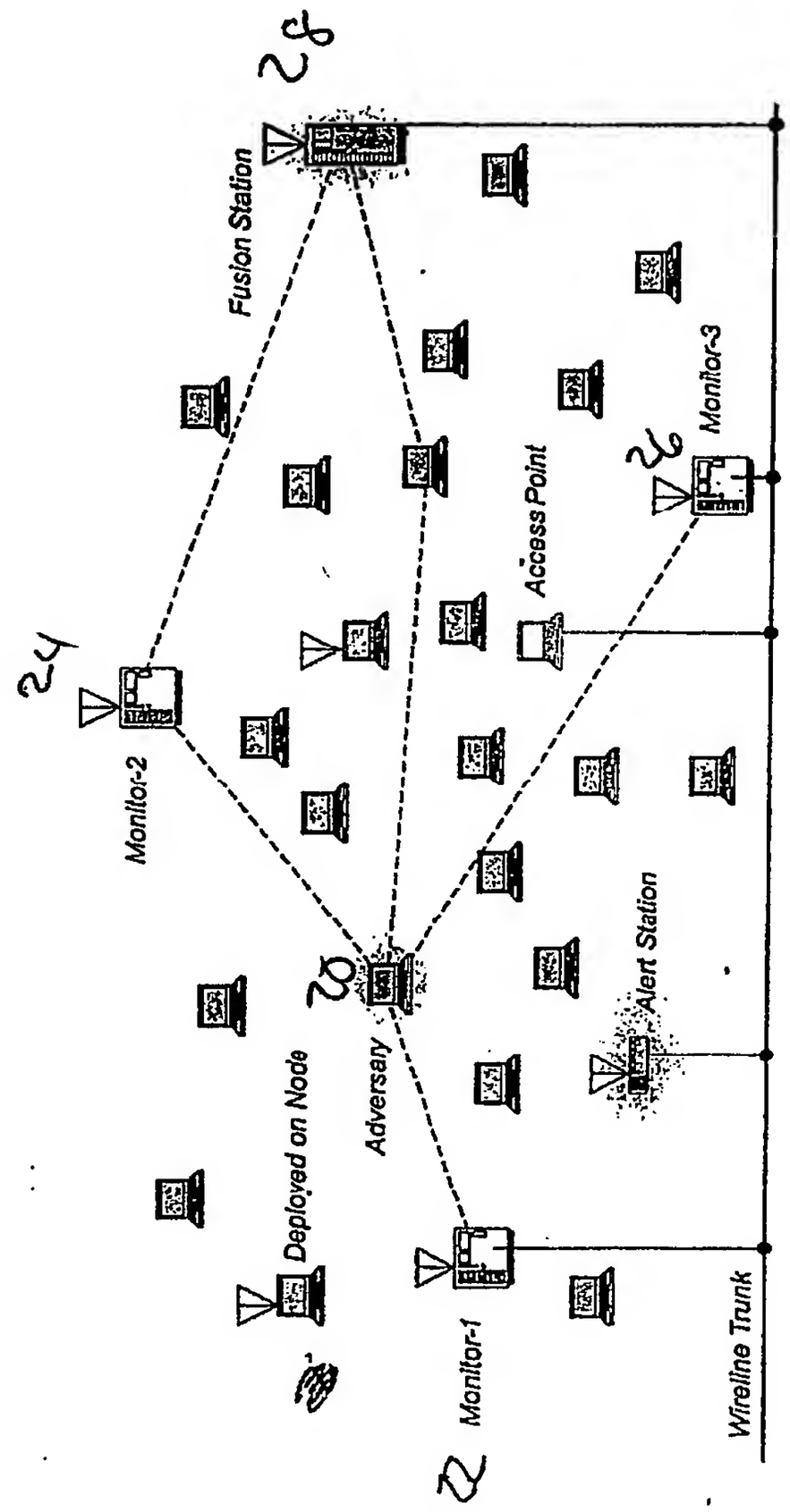
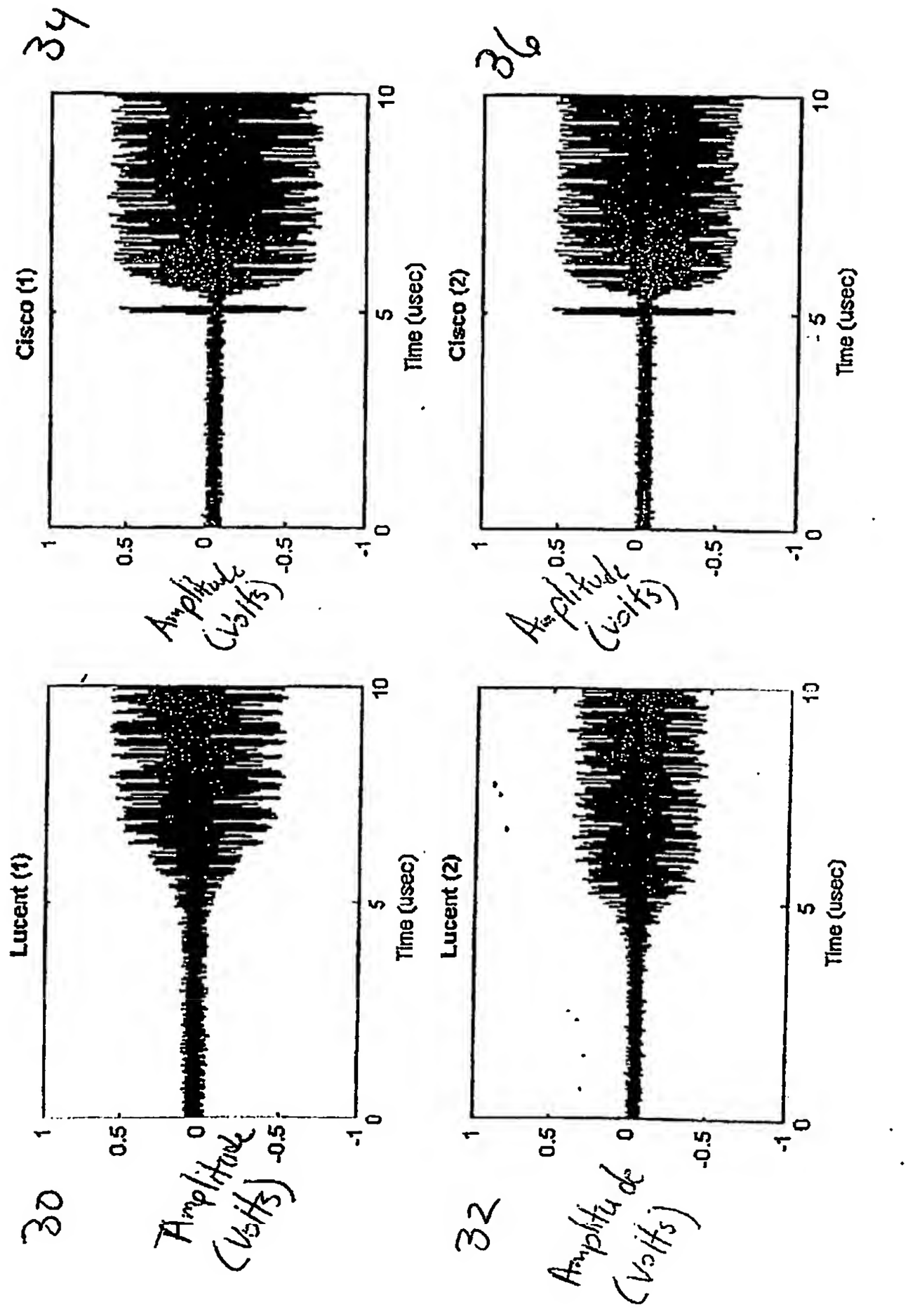


FIGURE 2



All 802.11b synchs and headers are transmitted using 1 Mbps DBPSK

FIGURE 3

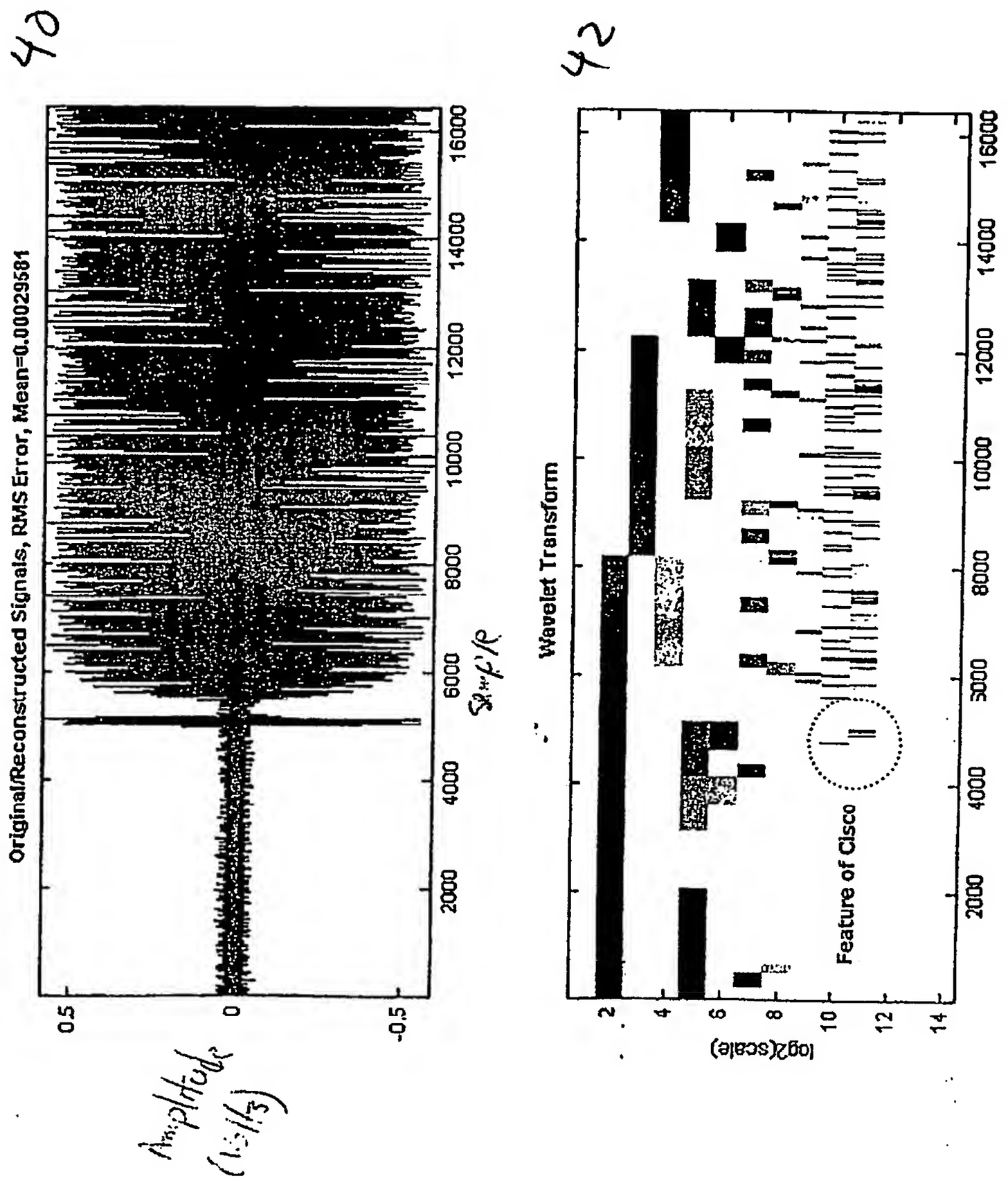


FIGURE 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/11107

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04B 17/00.
US CL : 455/67.11, 67.13, 456.1, 556.1, 557; 370/245, 902, 903

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/67.11, 67.13, 456.1, 556.1, 557; 370/245, 902, 903

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,266,350 B1 (OJARD et al) 24 July 2001, col. 4, lines 6- 63; col. 8, line 7-63	1-19
Y	US 6,253,064 B1 (MONROE) 26 June 2001, col. 7, line 6-col. 8, line 39; col. 17, line 38- col. 18, line 62.	1-19
Y	US 5,682,142 A (LOOSMORE et al) 28 October 1997, col. 3, line 39- col. 4, line 45; col. 5, line 6- col. 6, line 44.	1-19
A	US 6,362,778 B1 (NEHER) 26 March 2002, col. 7, line 15- col. 8, line 19.	1-19
A	US 5,027,383 A (SHEFFER) 25 June 1991, col. 4, line 8- col. 5, line 6; col. 7, line 26- col. 8, line 56.	1-19

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2003 (15.06.2003)	07 JUL 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Vivian C. Chin Telephone No. 703-308-6739

Form PCT/ISA/210 (second sheet) (July 1998)